RSAC 2025 Conference

Many Voices.
One Community.

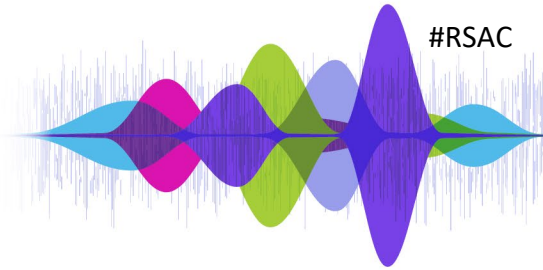
SESSION ID: SAT-W02

Widening Our Lens on OSS Security: People, Practice, and Partnership

Dr. Kelley Misata

President | Chief Trailblazer
Open Information Security Foundation (Suricata) | Sightline Security
https://www.linkedin.com/in/kelley-misata-ph-d-38475636/

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

OISF SURICATA

RSAC 2025 Conference

Open Source is growing…

- **As a valued resource ->** *without OSS… firms would pay an estimated 3.5 times more to build the software and platforms that run their businesses.*
- **As an integrated part of systems and technology ->** 70-90% of any given software code base consists of OS elements.
- **In complexity and use ->** OS solutions are part of global internal security systems either knowingly or not.
- **With more contributors and projects ->** 5.2+ billion GitHub contributions to more than 518 million OS, public, and private projects in 2024.
- **In market size ->** from $41.83 billion (2024) -> $48.92 billion (2025).

https://octoverse.github.com
https://www.library.hbs.edu/working-knowledge/open-source-software-the-nine-trillion-resource-companies-take-for-granted
https://www.ibm.com/think/topics/open-source
https://www.thebusinessresearchcompany.com/report/open-source-software-global-market-report

OISF SURICATA

But there is still a lot of "mystery"…

A bit about me…

- President, Open Information Security Foundation (Suricata)
- Chief Trailblazer, Sightline Security
- Open Source Advisor and Board Member, Tenzir
- (former) Senior Director of Open Source, Corelight
- (former) Director of Communications, Tor Project
- Ph.D in Cybersecurity, Purdue University

OISF SURICATA

Looking Beyond the Myth

- **What People Think vs. What's True**
  - Often romanticized as a community of friendly coders working together for the common good.
  - Reality -> t's complicated—people, governance models, business interests, licensing restrictions, and security risks.
  - Securing OSS isn't just about the code—it's about the entire ecosystem that surrounds it.
- **Why This Should Matter to You**
  - OSS is everywhere—may organizations don't know how to harness it.
  - OSS is part of the supply chain—understanding how it actually works is essential for making good security decisions.

People - Practices - Partnerships

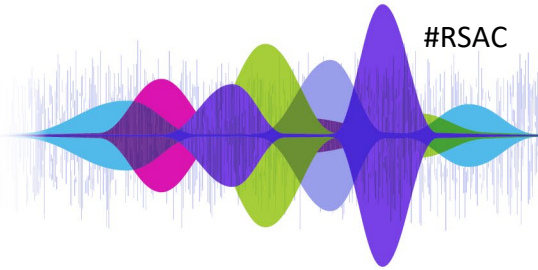
RSAC 2025 Conference

PEOPLE
The Humans Behind the Code

The *messy* part!

Many Voices.
One Community.

Start with the “who” – not the band!



- OS depends on a wide array of people from big-name companies to unpaid maintainers.
- Reasons people start an OS project varies – as does their own motivation for monitoring and maintaining it.
- It is not all developers, people across disciplines are part of open source.
- Often succession planning isn’t ”a thing” – how to deal with the **bus factor.**
- and most importantly….

Open Source doesn't [always] mean

"Community" Driven

RSAC 2025 Conference

PRACTICES
More than Code – Looking Wider

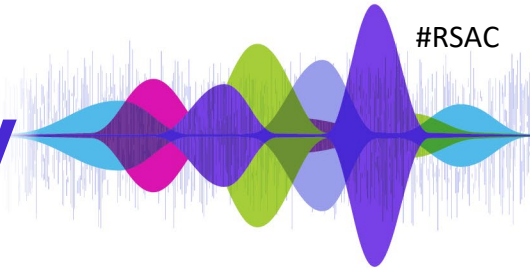
Governance – Legal – Business Operations

Many Voices.
One Community.

Governance: who makes the decision?

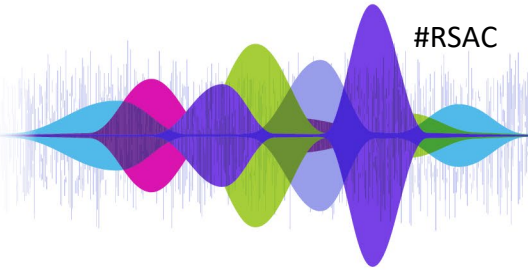
- **OSS isn't a democracy**—different projects have different power structures, and some none at all.
- **Different models mean different things**—do-ocracy, benevolent dictator for life, self-appointing councils or foundations, vendor-controlled
- **Enterprise due diligence**—maintenance, sustainability, leadership
- **Balancing the "spirit" of open source**—strategic lever, business priorities, "smoke and mirrors," internal conflicts, and more.

Legal: Licenses, Restrictions, and Security



- **Licensing isn't just legal red tape**—it shapes the project in many ways: use, modifications, sustainability, security.
  - MIT, Apache 2.0, BSD – permissive-> few restrictions, but little control over security
  - GPL – restricted-> requires code-sharing, some avoid it due to legal complexity
  - Business Source License (BSL) & Source-Available Model-> protest business interests but aren't truly OS.
- **Security risks in licensing incompatibility**—some knowingly combine OS components under conflicting licenses
- **Lack of enforcement**—difficult for many projects keep on top of violators.

Operations: Business Interests Behind OSS



- **OS isn’t always a passion project**—it is often driven by business goals, sponsorships, etc.
- **Security and sustainability tradeoff**—keeping funding going and business priorities.
- **New technologies**—AI-generated OS code introduces new concerns around security as well as opportunities.
- **Contingency planning**—how reliant is your organization (product or infrastructure) on OS? Do you have a back up plan?

RSAC™ 2025 Conference

If you require high security from OSS, are you investing in the projects you use?

Many Voices.
One Community.

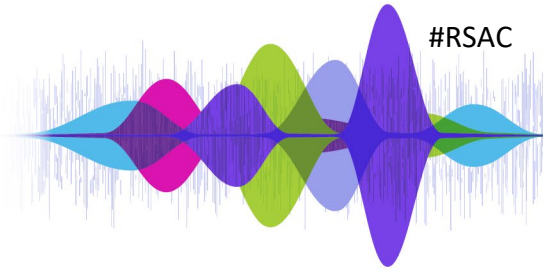
RSAC | 2025 Conference

PARTNERSHIPS
Securing Open Source Software

**The future isn't just about individual projects—
it's about the ecosystem.**

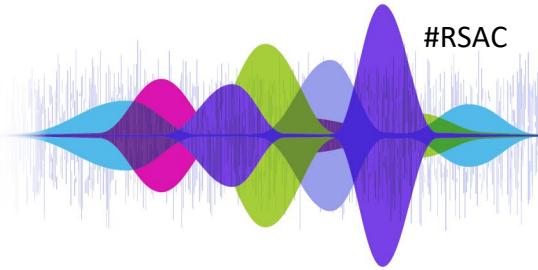
Many Voices.
One Community.

Finding Ways to Play Well Together: OS Projects, Enterprises, and Government



- Open source is a shared resource, but no single entity is fully responsible for its security.
- “Communities” can be seen, measured, and heard, don’t assume they always exist.
- The biggest users of OSS (governments & corporations) contribute the least.
- Guardrails make some feel better–-what is the risk to the foundational tenants of open source?

Thinking Towards the Future



- Building trust, conversation and collaboration is an evolving process not a destination.
- Not all OS projects are the same, therefore the partnerships with large enterprises and governments will be different.
- Navigating advancing technologies (e.g. AI, LLMs, ML) through the eyes of OS is shifting the conversation(s).
- OS isn't a *nice to have*, it's deeply embedded across the technology stack.
- OSINT and other resources growing in popularity to help manage risks.

RSAC™ 2025 Conference

Let's Apply It…
Adopt a New Mindset Today

People, Practices, and Partnerships

Many Voices.
One Community.

Reframe your own thinking... and share!

- **Security Requires More Than Just Code Fixes**
  - It's shaped by who runs the project, how it's governed, and how it's funded - find out who maintains it, how it's funded, what happens when things go bad.
- **Build in OS Due Diligence**
  - Before adopting OS, do your homework - ask yourself and the project hard questions about governance, funding, and sustainability.
- **Take a Seat -- Get Involved in OS Beyond Just Using It**
  - Support OS through direct funding, hiring maintainers, contributing code, volunteer your expertise, join working groups, initiatives, and OSS governance discussions.

What to start with today…

- **ASK:** What OS tools does our organization rely on? Start the conversation internally.
- **EMBRACE:** The OS mindset—think about governance, security, and sustainability.
- **PLAN:** What if a critical OS component disappears tomorrow? How would that impact your organization?
- **RETHINK:** If OS is part of your software supply chain, how does that shift internal risk and procurement discussions?
- **ENGAGE:** Reach out to project owners and maintainers—many are eager to collaborate with users and integrators.

AND….

RSAC™ 2025 Conference

Recognize that every open source project is different and the security of it is a shared responsibility—

it requires commitment, not just consumption.

Many Voices.
One Community.

TRUST

(and confidence)
comes with knowing
who's behind the code.

OISF SURICATA

RSAC 2025 Conference

Many Voices.
One Community.

Questions and Thank You!

Let's Connect: Dr. Kelley Misata

Join the Suricata community: https://suricata.io/